CLAIMS

We Claim:

1. A smart card device comprising:

   a controller;

   a smart card reader in communication with said controller;

   a communications interface coupled to said controller; and

   a power source.

2. The smart card device according to claim 1, configured to be connectable between a telephone and the wall socket of a telephone line.

3. The smart card device according to claim 1, configured to be connectable to a cellular telephone.

4. The smart card device according to claim 1, wherein said communications interface comprises at least one of a group including a MODEM, Ethernet, infra-red (IR), RF and audio tones.

5. The smart card device according to claim 1, further comprising:

   a display screen; and

   a numeric and/or functions keypad.

6. The smart card device according to claim 1, further comprising:

   encryption means.

7. The smart card device according to claim 1, wherein said power source comprises at least one energy source from a group including an internal battery, an external power inlet, the communication media to which the device is coupled and a rechargeable battery.

8. The smart card device according to claim 1, further comprising a connector for external devices, said external devices comprising any of a group including a printer, a keypad and a biometric data reader.

9. The smart card device according to claim 1, further comprising at least one of a group including a printer, a keypad and a biometric data reader integrated within the device.

10. The smart card device according to claim 1, wherein said smart card reader further comprises at least one of a group of processing components including a additional computation capabilities, additional communication interfaces and additional encryption capabilities.

11. The smart card device according to claim 1, wherein said smart card reader further comprises at least one memory component, said at least one memory component comprising at least one of a group including Read Only Memory (ROM), Non-Volatile Memory (NVM) and Random Access Memory (RAM).

12. A system for remotely verifying the identification (authentication) of the user of a smart card, the system comprising:

a smart card device, comprising:

a controller;

a smart card reader in communication with said controller;

a communication network interface coupled to said controller; and

a power circuit, and

a remotely located server in communication with said communications interface comprising means for verifying the validity of the smart card being read by said smart card device or other data keyed into said device.

13. The system according to claim 12, wherein said remotely located server further comprising means for validating a certificate or generating a "challenge" and accepting the "response" for said challenge.

14. The system according to claim 12, wherein said other data comprises at least one of a group including a personal identification number (PIN) and biometric data.

15. The system according to claim 12, wherein said smart card device is configured to be connectable between a telephone and the wall socket of a telephone line.

16. The system according to claim 12, wherein said remotely located server is any one of a group including an Internet server and an Interactive Voice Recognition server (IVR), or a Point Of Sale (POS).

17. The system according to claim 12, wherein said communications interface is at least one of a group including a MODEM, Ethernet, infra-red, RF, and audio tones.

18. The system according to claim 12, wherein said smart card device is configured to be connectable to a cellular telephone.

19. The system according to claim 12, wherein said smart card device further comprises:

a display screen; and

a numeric and/or functions keypad.

20. The system according to claim 12, wherein said smart card device further comprises:

an encryption module.

21. The system according to claim 12, wherein said power source comprises at least one energy source from a group including an internal battery, an external power inlet, the communication media to which the device is coupled and a rechargeable battery.

22. The system according to claim 12, wherein said smart card reader further comprises at least one of a group of processing components including an additional computation capabilities, additional communication interfaces and additional encryption capabilities.

23. The system according to claim 12, wherein said smart card reader further comprises at least one memory component, said at least one memory component comprising at least one of a group including Read Only Memory (ROM), Non-Volatile Memory (NVM) and Random Access Memory (RAM).

24. The system according to claim 12, wherein said remotely located server further comprises means for transferring e-goods or e-money.

25. A method for verifying the identification of the remote user of a smart card, the method comprising the steps of:

inserting a smart card into a smart card device, said smart card device comprising:

a controller;

a smart card reader in communication with said controller;

a communications interface coupled to said controller; and

a power source;

transmitting data from the smart card, via said communications interface, to a remotely located server;

inputting privately known information into said smart card device and transmitting said proof of signature (certificate) to said remotely located server; and

said remotely located server verifying that said privately known information is a valid one for the card.

26. The method according to claim 25, wherein said privately known information comprises at least one of a group including a personal identification number (PIN) and biometric data, or other personally known information.

27. The method according to claim 25, wherein said device contains a power source, said power source comprising at least one energy source from a group including an internal battery, an external power inlet, the communication media to which the device is coupled and a rechargeable battery.

28. The method according to claim 25, wherein said device also contains encryption means.

29. The method according to claim 25, wherein said remotely located server transfers transaction information to said smart card device for approval.

30. A method for remotely purchasing goods or services, the method comprising the steps of:

inserting a smart card into a smart card device, said smart card device comprising:

a controller;

a smart card reader in communication with said controller;

a communications interface coupled to said controller; and

a power source;

selecting an item to be purchased from a supplier;

transmitting data read from the smart card, via said communications interface, to a remotely located server in communication with said supplier;

said remotely located server transferring transaction information associated with the purchase to said smart card device for approval; and

storing said transaction information in said smart card.

31. The method according to claim 30, further comprising the step of authenticating the identity of the smart card user.

32. The method according to claim 30, wherein said step of authenticating comprises the steps of:

inputting privately known information;

said smart card verifying that said privately known information matches the smart card data; and

generating a certificate validating the transaction.

33. The method according to claim 32, wherein said privately known information comprises at least one of a group including a personal identification number (PIN) and biometric data.

34. The method according to claim 32, wherein said step of authenticating is performed by said remotely located server.